GOVERNMENT OF PUERTO RICO
DEPARTMENT OF PUBLIC SAFETY
Puerto Rico Police Bureau

ALEXIS TORRES
SECRETARY

ANTONIO LÓPEZ FIGUEROA
COMMISSIONER

COMMONWEALTH OF PUERTO RICO AND PUERTO RICO POLICE BUREAU IT CORRECTIVE ACTION PLAN

March 31, 2023

TABLE OF CONTENT

IT Corrective Action Plan

1.0 INTRODUCTION AND BACKGROUND

The following Information Technology (IT) Corrective Action Plan sets forth the steps the Commonwealth of Puerto Rico and the Puerto Rico Police Bureau (PRPB) will take to ensure its IT systems and solutions meet the needs of its employees and the community they serve. This IT Corrective Action Plan is also intended to support the Commonwealth's implementation of the Agreement for the Sustainable Reform of the Puerto Rico Police Bureau ("Consent Decree"), entered in *United States v. Commonwealth of Puerto Rico*, No. 12-cv-2039 (FAB), on July 17, 2013.

On April 18, 2022, the Court entered a stipulated order on IT providing for a comprehensive IT needs assessment and action plan to comply with the Consent Decree "in a timely, efficient, and cost-effective manner." ECF No. 2000 at 1. As part of the stipulated order, the Court endorsed the Parties' agreement and observed that an "adequate needs assessment and action plan are necessary to address the Monitor's compliance findings, address PRPB's critical IT needs, and chart a path toward sustainable reform that is consistent with the [Consent Decree] and the Commonwealth of Puerto Rico's public safety goals." *Id.*

In accordance with the stipulated order, in fall 2022, the Commonwealth, in conjunction with the Court Monitoring Team, engaged Gartner Consulting to assess PRPB IT practices, processes, capabilities, and systems. Gartner submitted its final Current State Assessment Report on 01 December 2022 and identified significant gaps and deficiencies. Ultimately, Gartner found that the identified issues "inhibit operational efficiency, undermine confidence in data and analytics, obscure operational performance and interactions with the public, sub optimize technology investments, and present risk to officer safety." (*See* Ex. 1, Current *State Assessment Report*, pg. 4, 01 Dec. 2022.)

Subsequently, the Commonwealth and PRPB engaged in workshops with Gartner to ultimately develop an IT Strategic Plan (*See* Ex. 2, *IT Strategic Plan and* Recommendations *Report*, 17 March 2023). The content of the *IT Strategic Plan and Recommendations* has served as the basis for the following IT Corrective Action Plan and the steps included herein.

This IT Corrective Action Plan will be updated at least once per year to ensure any new IT initiatives related to Consent Decree implementation and/or compliance are incorporated herein.

A. Imperative Corrections

The plan contained herein addresses IT needs identified as the highest priority initiatives for action that represent the greatest benefit for the Commonwealth, PRPB, and its

IT Corrective Action Plan (Draft)

citizens. The following are focus areas that demand remediation and immediate corrective actions.

- **Implement a contemporary Best Practices Governance Oversight and Management Protocol comprised of accountable leadership, top-down, from the Commonwealth Department of Public Safety to oversee, manage, guide, direct and make decisions to enact this corrective action plan** – Threshold; map and institutionalize roles and responsibilities, organizational and decisional hierarchies no later than 01 July 2023.

- **Upgrade data and infrastructure networks and provide fullest possible wireless/digital access to information, data, systems, applications, and tools –** Threshold; 95% endpoint access NLT 31 Oct 2023. Goal 100% endpoint access implemented NLT 31 Mar 2024.

- **Maximize radio handset inventory and improve network coverage** – Threshold; 90% handheld radio availability measured operationally at each precinct/operational unit implemented NLT 30 Sep 2023. Goal – 100% radio availability operationally at all times implemented NLT 31 Mar 2024.

- **Resolve IT organizational and resourcing needs** – Threshold/Goal; 100% staffing, including technology subject matter experts and contractors per a fully vetted IT staffing plan to be prepared no later than 31 July 2023 and implemented NLT 30 Sept 2024.

- **Update technology at the Training Academy** – Threshold; Per Academy Support Plan to be prepared no later than 30 April 2023 and implemented NLT 31 Dec 2024.

- **Maintain an equipment refresh lifecycle enterprise wide** – Threshold; Per IT Support Plan to be prepared no later than 30 June 2023 and implemented NLT 30 June 2024.

- **Institutionalize data and analytics capabilities and continue process improvement activities** – Threshold; Baseline and document essential data and tradecraft skills (in partnership with AH-Datalytics) NLT March 2022. Goal; Re-baseline essential and critical data and tradecraft skills (in partnership with AH-Datalytics) NLT 31 Dec 2024.

- **Suspend GTE development unless operationally essential** – Threshold; Baseline requirements and specifications for replacement of GTE NLT 31 May 2023.

- **Implement a modern Law Enforcement Records Management System** – Threshold; Conduct market analysis NLT 30 September 2023, Implement GTE Replacement, Version 1.0 no later than 30 June 2024.

- **Improve mobile infrastructure to meet operational needs for broadest possible access to data and technology tools necessary for field operations endpoint situational awareness** – Threshold; plan and scope a mobile access architecture NLT 30 September 2023, Goal; Implement the plan NLT 31 December 2023.

IT Corrective Action Plan (Draft)

B. The Commonwealth's Commitment

The Commonwealth is committed to successfully implementing this IT Corrective Action Plan. This includes allocating the funding and resources necessary to bring this plan to fruition, consistent with Paragraph 289 of the Consent Decree.

This IT Corrective Action Plan is designed to strengthen and support IT Governance and resourcing at PRPB to address the current limited IT capacity of PRPB. The Commonwealth commits to provide or obtain sufficient funding and resources to implement each initiative to promote compliance with the Consent Decree and ensure sustainability of reforms.

2.0 CONSENT DECREE REQUIREMENTS

The implementation of this Corrective Action Plan will support the Commonwealth's efforts to achieve substantial compliance with the IT requirements of the Consent Decree (Paragraphs 218-224).   Implementation will also promote compliance with other requirements in each of the other ten substantive areas of the Consent Decree, as set forth in Appendix A.

3.0 IT GOVERNANCE

Supporting the development and implementation of that IT vision should be a formal IT governance structure to help set and manage priorities. Clear lines regarding IT governance are critical to the operation of a public safety agency, as IT serves as the foundation for all operations, including mission-critical communications, accurate reporting, investigations, management, and transparency. Without a proper governance structure that includes both IT staff and business owners, IT is often misaligned with the business, is implemented in an IT "vacuum", and is rarely successful.
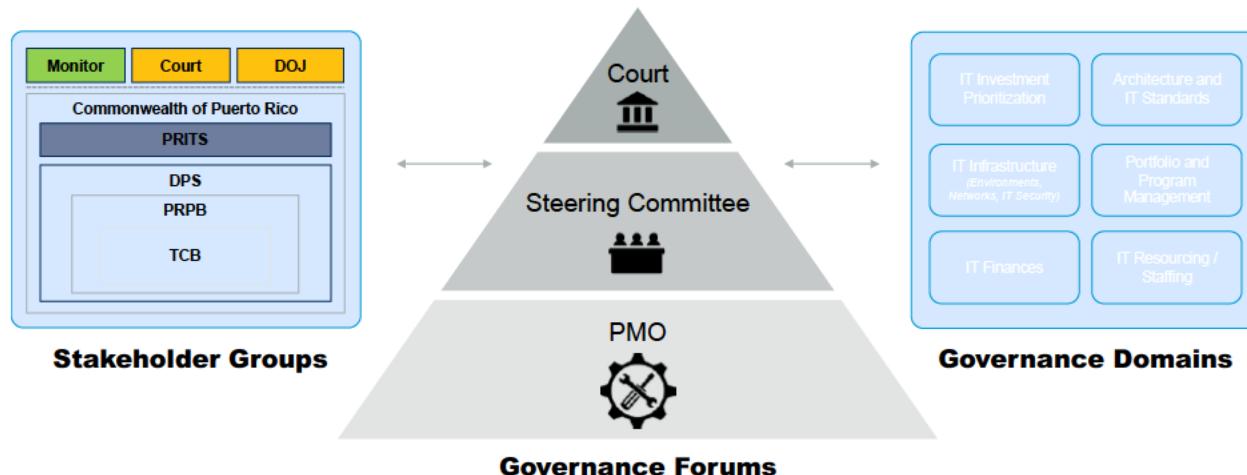
IT Corrective Action Plan (Draft)

A governance structure that allows leadership to define operational goals and objectives, and ensure that all IT initiatives directly support those goals is key to successful IT. A proper IT governance structure should enable sound IT decisions making, ensure silos are not created, advocate for proper funding, plan for ongoing training and education, develop proper policies, and work to understand the needs and requirements of its users. Such a structure should also enable leadership to reprioritize initiatives as new or unexpected priorities arise. The proper implementation of this IT Corrective Action Plan will ensure that such a governance structure remains in place for the future benefit of the Commonwealth beyond the life of the Consent Decree.
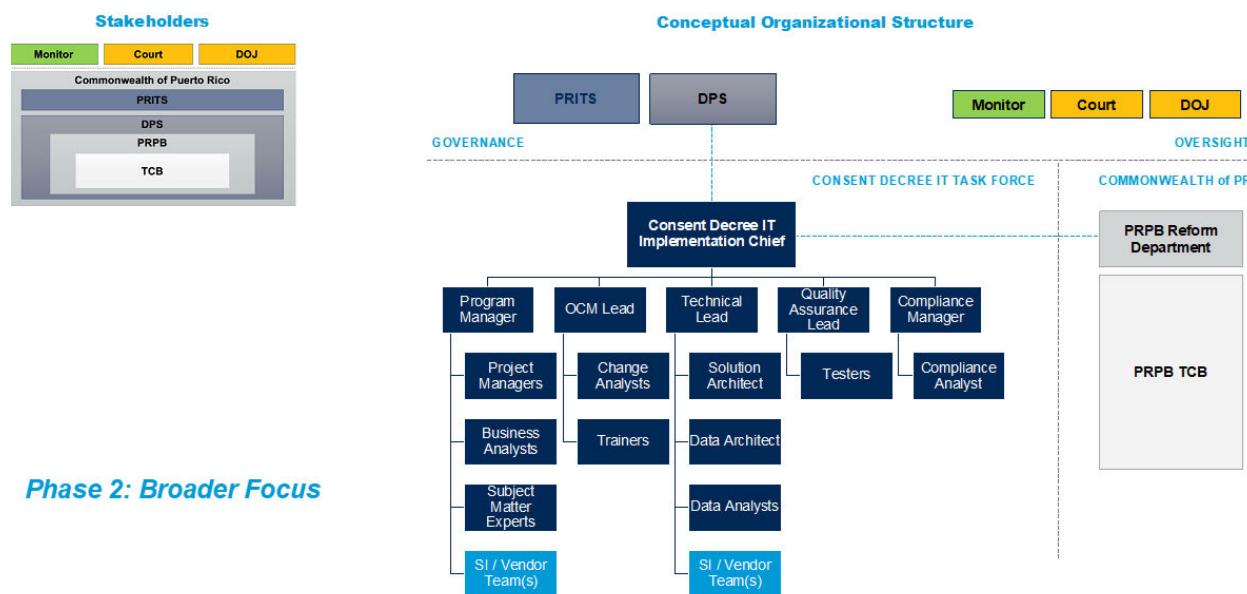
A. Executive Level Governance

An executive level steering committee, comprised of leadership from various areas across the Commonwealth and the Department of Public Safety (DPS), should set and oversee priorities for IT needs, ensuring all long-term plans for technology and data are in line with PRPB's operational goals and objectives.

1. Executive Level IT Planning Committee

The Commonwealth has established an executive -level IT Planning Committee ("IT Planning Committee") to ensure that all IT initiatives will directly support the goals and objectives of PRPB. The IT Planning Committee is led by the Executive Director of the Puerto Rico Innovation and Technology Service ("PRITS"), or her

IT Corrective Action Plan (Draft)

designee, and the Secretary of DPS, or his designee. It is also comprised by representatives from PRPB and other Commonwealth agencies.

The initial members of the IT Planning Committee are:

Voting Members

1. PRITS Interim Director (currently, Nannette Martínez Ortiz)
2. DSP CIO (currrently, Juan C. Rivera Vázquez as interim CIO)
3. Governor' Secretary Office for the Innovation, Data and Technology (currently, Enrique Volckers Nin)
4. PRPB, Director of Reform Office (currently, Lt. Coronel Rolando Trinidad Hernández)
5. Governor's Representative (currently, María del Mar Ortiz Rivera)
6. Office of Budget/Finance, Director (currently, Juan C. Blanco)

Advisory Members

- PRPB CIO and Director of the Technology and Communications Bureau
- PRPB Communications Division Director
- PRPB Technology Division Director
- Program Manager and PMO Personnel
- IT Innovation Task Force Personnel

The IT Planning Committee will ensure initiatives are prioritized to directly support the needs of PRPB's work units and strategic priorities, ensure data silos are not created, advocate for proper funding, ensure the necessary resources are in place, review and approve IT use policies, and ensure proper training and education is provided for all users of IT across PRPB. The IT Planning Committee will also prioritize all IT initiatives and reprioritize initiatives as new or unexpected priorities arise.

a. Meeting and Reporting
The IT Planning Committee will **meet monthly** to receive a status report and briefing from the Program Manager and Project Management Office, and to take action as necessary to ensure the success of the IT Corrective Action Plan.

The IT Planning Committee will hold a **monthly meeting with the DOJ and Monitor** to provide the status of all IT initiatives.

The IT Planning Committee will file a **90-day Status Report** with the Court once each quarter to provide the Court with:

IT Corrective Action Plan (Draft)

1. A description of tasks completed over the past 90-day period;
2. An explanation regarding and tasks in the Corrective Action Plan that have been delayed, including a plan to remedy any delays;
3. A description of tasks to be initiated and/or completed over the next 90-day period;
4. A chart or charts depicting the current status of each task in the Corrective Action Plan; and
5. A description of any risks and/or challenges that may potentially impact the success of the Corrective Action Plan, and a plan to remediate those risks.

B. Program Level Governance

Any technology initiative must include a clear governance structure to ensure best practices are followed for the planning, implementation, and support of each technology or data system initiative. When IT initiatives fail, it is often not due directly to failures in the technology itself; rather, failures are often the result of gaps in the planning, management, and governance of the technology initiative.

1. Program Management

A Program Manager will be hired/contracted to ensure all IT initiatives are managed according to best practices. The Program Manager will have expertise in IT Governance and program/project management, and will report up to Executive Level IT Planning Committee. The Program Manager will:

- Directly manage the Project Management Office as well as the Project Manager assigned to lead the IT Innovation Task Force.
- Coordinate efforts across all IT initiatives
- Oversee the creation of status reports, project schedules, and other project management artifacts
- Ensure all project managers follow best practices in tracking resources, costs and schedule for their respective projects.
- Report the status of the Corrective Action Plan and all Consent Decree related/supportive IT initiatives to the Executive Level IT Planning Committee, identifying risks and challenges, and requesting necessary assistance/resources.

C. Project Level Governance

1. Project Management Office

PRPB will establish a Project Management Office (PMO), that reports to the

8

IT Corrective Action Plan (Draft)

Program Manager, to manage IT projects. The PMO will provide a combination of oversight, delivery management and implementation process compliance over both ongoing PRPB owned IT initiatives and the IT initiatives owned by the IT Innovation Task Force.

This essentially represents how IT governance within PRPB operates today, with a central IT team at headquarters that works in partnership with regional IT resources. Both the PRPB IT organization and the newly to-be established IT Innovation Task Force participate together with the PMO to ensure cross-portfolio coordination and planning, and in turn, report into the Program Manager.

The PMO will be responsible for:

a. Performance Management

   Active monitoring of projects using indicators that ensure the effective, timely and delivery of services, with the identification of deficiencies on a weekly basis.

b. Risk Analysis

   Identification, assessment and prioritization of risks and controls that ensure appropriate visibility and oversight in the management of risks to IT projects (risks include, but are not limited to, data and information security, operational results, financial, staffing, vendors and capital projects).

2. IT Innovation Task Force

   Due to the urgency of the Consent Decree IT requirements regarding records management and data collection/analysis, the IT Innovation Task Force is being established as a separate organization from PRPB IT to eliminate on-going IT support distractions. The IT Innovation Task Force will report to the Program manager, and then to DPS CIO administratively. The new IT Innovation Task Force will have its separate budget, as well as staffing and purchasing authority to the extent possible to provide adequate resources and expedite progress on achieving compliance with critical Consent Decree IT requirements.

   Initially, the IT Innovation Task Force will own the RMS implementation initiative. Resources, staffing / skills, and organizational constructs will be implemented with this immediate, sole, objective in mind. Through the RMS implementation, the IT Innovation Task Force will mature and will then be able to scale up to take responsibility for other Consent Decree related strategic IT initiatives, and

9

IT Corrective Action Plan (Draft)

ultimately, any large-scale IT effort focused on modernization and sustainability of IT.

Upon completion of the Consent Decree IT requirements (or a significant portion thereof), PRPB and the Commonwealth will merge the IT Innovation Task Force back into PRPB IT, to leverage the resource capacity and best practices developed within the task force to sustain long term IT success within PRPB.

3. Project Working Groups

PRPB will establish a working group for each IT initiative. The working groups will be responsible for developing detailed implementation plans for their respective initiative(s), and will work with the PMO to ensure successful implementation of IT initiatives. Upon approval of the implementation plans, the working groups will be responsible for implementing their initiative, including conducting system testing, and developing policies and training curricula and materials for DOJ and Monitor approval. Ultimately, the working group members will serve as subject matter experts for their IT initiative and may serve as instructors for system training (if they are qualified instructors) and as level 1 support for end users.

The Working Groups will define user needs and functional business requirements, work with IT resources to understand what capabilities or improvements are possible, communicate those user needs and business requirements to the appropriate IT resources, and then serve as subject matter experts to test new systems and capabilities to ensure they meet the needs of the business. They may also help provide input into use policies and procedures, and may serve in a "train-the-trainer" capacity during deployment of the new technology, as appropriate.

IT Governance Task List

Task	Description	Due Date	Status
1.	Hire SME to help facilitate governance process and to serve as Program Manager, create documentation (including Governance Oversight and Management Protocol), and facilitate initial IT Planning Committee and PMO meetings	01 JUL 2023	Planning Phase
2.	Hold first IT Project Management Office meeting	07 APR 2023 and then weekly	Planning Phase
3.	Hold IT Planning Committee meeting	14 APR 2023 and then monthly	Not Started

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
4.	IT Project Management Office submits first monthly status report to IT Planning Committee	08 MAY 2023 and then monthly	Not Started
5.	IT Planning Committee submit first 90-Day Status Report to Court	01 JUL 2023 and then quarterly	Not Started
6.	Establish IT Innovation Task Force	30 SEP 2023	Planning Phase
7.	Enhance PMO staffing	30 SEP 2023	Planning Phase

4.0 IT PRIORITIES

The following seven IT initiatives have been identified by the IT Planning Committee.

The task lists contained in this Corrective Action Plan are only a starting point. PRPB will establish teams for each initiative that will focus on hiring/contracting with SMEs with the appropriate skill sets to develop and lead detailed implementation plans for each initiative.

Further, a collaboration period will be included for each initiative to allow for stakeholder review and approval of each detailed implementation plan.

A. IT Resourcing/Staffing

The Commonwealth and PRPB will hire and/or contract with the resources necessary to successfully implement this IT Corrective Action Plan.

Without the proper IT resources and staff, PRPB will not be able to successfully implement even a portion of this IT Corrective Action Plan. IT resources are required from both a technical perspective (network and server support, database management, cyber security, etc.), and an end user perspective (system administration, help desk support, user access administration, IT system training, etc.)

The following chart summarizes the IT Resourcing initiative and the Steps PRPB will take to implement the initiative.

Initial Tasks and Timing – IT Resourcing/Staffing

Task	Description	Due Date	Status
1.	Review the current inventory of active and planned projects and suspend work on projects that are not essential or do not align with the IT Corrective Action Plan priorities.	31 MAY 2023	In process
2.	Monitor and DOJ review and approval of active, planned and suspended IT projects.	31 MAY 2023	Not started
3.	Assess current PRPB IT skillsets, and Identify gaps in the skillsets that need to be filled.	30 JUN 2023	Not started

11

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
4.	Develop an IT staffing plan to provide role clarity, hire, contract and reassign resources to support IT Corrective Action Plan.	31 JUL 2023	Not started
5.	Hire all necessary staff and contractors.	30 SEP 2023	Not started
RMS Staffing - IT Innovation Task Force			
1.	Create a dedicated team to appropriately staff the IT Innovation Task force to complete the Records Management System / GTE Replacement	31 JUL 2023	Planning phase
2.	Establish a Records Management / GTE Replacement SME team	31 JUL 2023	Planning phase
3.	Utilize a Business Analyst to work with the SME team to gather requirements and tailor a scope statement	31 AUG 2023	Not Started
4.	Acquire and/or reassign staff to support the RMS/GTE Replacement initiative, including the positions outlined in Tasks 5-10, below.	31 JUL 2023	Planning phase
5.	Project Manager to oversee and drive the implementation	31 AUG 2023	Not Started
6.	Integrations Architect to build required integrations	31 AUG 2023	Not Started
7.	Data Engineer to oversee data conversion,	31 AUG 2023	Not Started
8.	Quality Assurance Analysts to test and ensure functionality is aligned with requirements	31 AUG 2023	Not Started
9.	Training Specialist to create an onboarding and training program for employees	31 AUG 2023	Not Started
10.	Various IT administrators to assist in rolling out the project	31 AUG 2023	Not Started
11.	Secure contracted services where additional resources are needed	31 AUG 2023	Planning phase
Network Staffing			
1.	Establish a team to facilitate network improvements, including the positions outlined in Tasks 2-3, below.	31 JUL 2023	Not Started
2.	Project Manager to organize, plan and execute the network plan	31 AUG 2023	Not Started
3.	Network Engineer to analyze, troubleshoot and evaluate network issues	31 AUG 2023	Not Started

The Commonwealth worked with Gartner to create the following high-level staffing recommendations for the initiatives in terms of role types and estimate level of effort in percentages of Full Time Equivalent (FTE) employees.

The Commonwealth will develop a more detailed staffing plan for each, closer to the time of each initiative starting. There are positions the Commonwealth must hire or contract with for its own project teams in addition to the roles / team any vendor will use to deliver their contracted scope of work.

IT Corrective Action Plan (Draft)

At a minimum, the following additional resources will be required for the top 7 IT priorities. The following list, however, is not exhaustive.

- Data Networks Initiative Staffing
  - Project Manager: 1 x FTE
  - Business Analyst: 1 x FTE
  - Network Engineer / Architect: 1 x FTE
  - Quality Assurance Analysts / Testers: 1 – 2 FTE during implementation
- Radio Networks Initiative Staffing
  - Project Manager: 1 x FTE
  - Radio Communications Specialist: 1 x FTE
  - Quality Assurance Analysts / Testers: 1 – 2 FTE during implementation
- RMS Initiative Staffing
  - Project Manager: 1 x FTE
  - Business Analyst: 1 x FTE initial, potentially up to 3 x FTE during implementation
  - Change Management Analyst: 1 x FTE
  - Solution Architect: 1 x FTE
  - Data Engineer / Data Management SME: 1 x FTE
  - Quality Assurance Analysts / Testers: 3 – 5 FTE during implementation
- Analytics and Reporting Staffing
  - Project Manager: 1 x FTE
  - Business Analyst: 1 x FTE
  - Data Engineer / Data Management SME: 1 x FTE
  - Quality Assurance Analysts / Testers: 1 – 2 FTE during implementation
- Mobility / Situational Awareness Staffing
  - Project Manager: 1 x FTE
  - Business Analyst: 1 x FTE initial, potentially up to 3 x FTE during implementation
  - Change Management Analyst: 1 x FTE
  - Solution Architect: 1 x FTE
  - Network Engineer / Architect: 1 x FTE
  - Quality Assurance Analysts / Testers: 2 – 3 FTE during implementation

The estimated cost[1] of the additional resources mentioned above for the top 7 IT priorities, to be in compliance with the plan implementation, is shown in the following table:

---

[1] Source: Glassdoor. Retrieved March 29, 2023, from https://www.glassdoor.com.

IT Corrective Action Plan (Draft)

Position	Qty	Salary/Year	Total
Program Manager	1	69,046.00	69,046.00
Project Manager	5	67,712.00	338,560.00
Business Analyst	8	62,633.00	501,064.00
Network Engineer	2	63,597.00	127,194.00
Quality Assurance Analyst/Testers	14	39,842.00	557,788.00
Radio Communication Specialist	1	49,757.00	49,757.00
Change Management Analyst	2	64,163.00	128,326.00
Solution Architect	2	86,834.00	173,668.00
Data Engineer/Data Management SME	1	69,950.00	69,950.00
Total	35		$2,015,353.00

Appendix B to this Corrective Action Plan includes the total number of IT staff that must be added to successfully modernize and properly maintain and support PRPB IT. The table shows both the current resources available to the Technology and Communications Bureau (TCB), as well as the amount and type of resources necessary to be sustainable in the implementation of project maintenance. Also, the table is synchronized with new and actual government employee job classifications. Funding necessary for the new human resource is **$3,252,000.00** annually recurrent for the new position.

B. Data Networks

PRPB will upgrade its IT data networks and provide wireless access across all PRPB facilities.

A data network is the foundation of all IT for all law enforcement agencies. A data network provides employees with access to the systems and information they need to do their job. A data network transports all data to and from the field, and across all PRPB locations. Without a proper data network, critical data cannot be accessed, submitted, or managed. A data network provides access to safety information that is critical to officer safety and community safety. A law enforcement agency cannot operate successfully without a reliable data network.

PRPB will improve its data network in two areas:

1. PRPB Facilities: The network that connects all of the PRPB buildings, offices and facilities.
2. PRPB Remote Network: The network that allows employees to access systems and information when they are out of the office (for example, an agent in their vehicle).

IT Corrective Action Plan (Draft)

The following chart summarizes the Data Networks initiative and the steps PRPB will take to implement the initiative.

Initial Tasks and Timing – Data Networks

Task	Description	Due Date	Status
Network Improvements for PRPB Facilities			
1	Request network vendor to develop a scope and budget for network improvements for the wired network.	30 APR 2023	Vendor identified, scope & quote requested
3	Request network vendor to develop a scope and budget for network improvements for the wireless network access points.	30 APR 2023	Vendor identified, scope & quote requested
3.1	Complete the Plan for the Redesign the integration of firewall perimeters to the network: a. Develop a network design with logic diagrams and routing strategy. b. Purchase ten 10GB SPF+ Optical Gigabit Ethernet Transceiver. c. Request service quote. d. Prepare a migration strategy for physical connections existing 1Gb copper to redundant 10Gb fiber aggregates for each firewall.	30 JUN 2023	Planning
3.2	Complete the Plan for Changes to the Centralized Network of Internet services to a Distributed Internet Network. a. Gathering information about the existing network, a network design document will be developed. b. Develop a network design with logic diagrams and routing strategy. c. Acquisition of network equipment (firewall, switch and router). d. Implementation of SD-WAN technology with decentralized architecture for Internet access. e. Configure la red WAN entre HQ y Claro se extenderá a una red /29. f. Deploy security appliance on the same logical WAN network and in parallel to CORE routers existing. g. Configure routing protocols at headquarters and command centers to handle the path selection for Azure and Internet. h. Install and configure the security appliance in the Command to	30 JUN 2023	Planning

15

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
	authenticate Internet access in the Cloud or HQ AD. i. Configure the Cloud in the Firewalls will handle the VPN and communications to HQ and command centers over VPN. j. Replace existing WAN routers with FortiGate appliances with SD-WAN		
4	Contract with network vendor for wired and wireless access point network improvements.	30 SEP 2023	Not started Depends on the Voice and Data contract.
5	Measure current state network performance attributes (upload / download rates in every facility)	31 OCT 2023	Not started
6	Implement necessary hardware upgrades (modems, routers, switches, cabling, etc.)	31 JAN 2024	On average a minimum of 60 days is required for equipment to arrive after purchase.
7	Measure post-implementation network performance attributes (minimally upload / download rates in every facility) to validate improved performance	29 FEB 2024	Not started
8	Oversee the completion of vendor implementation of the network improvements for PRPB facilities, of both wired networks and secure wireless network access points. Work with contracted vendor to report on network performance improvements realized	31 MAR 2024	Not started
Network Improvements for Remote Access			
1.	Supplement and formalize a project team with at least a project manager, technical / network specialist and business analyst.	30 SEP 2023	New hires/contractors
2.	Document requirements for wireless mobile (cellular) access to PRPB applications and systems using PRPB use cases (i.e., Agents in patrol vehicles, Investigators performing remote duties, Command staff managing incidents on-scene)	30 SEP 2023	Not started
3.	Identify cellular carrier that can provide secure remote access to PRPB network.	31 MAY 2023	Vendor identified, scope & quote requested
4.	Contract with identified cellular carrier	30 SEP 2023	Not started
5.	Conduct project planning with selected wireless mobile (cellular) service provider and prepare for the implementation stage.	30 SEP 2023	Not started

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
6.	Procure all necessary hardware and software (e.g., mobile vehicle routers)	30 SEP 2023	Not started
7.	Oversee the vendor and complete the implementation of remote network with required security and access.	31 DEC 2023	Not started

C. Radio Coverage

PRPB will improve the coverage of the radio network across the Commonwealth and ensure every agent has a working radio handset.
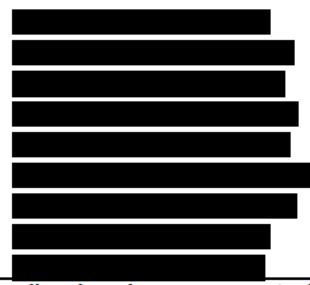
Robust radio coverage is mission critical for all law enforcement agencies worldwide. All agents must have a radio they can depend on one hundred percent of the time to ensure communications are truly reliable. Radio communications are critical to officer and civilian safety, as radios enable agents to call for backup, request a supervisor on scene, and request other emergency support (e.g., Specialized Unit, Fire, or EMS).

PRPB will improve its radio coverage in three areas:

1. Radio Network Coverage: PRPB will work with its vendor to replace all aging infrastructure for its radio network (e.g., amplifiers, repeaters, etc.) to provide a reliable radio network with coverage across all of Puerto Rico.
2. Portable Radios: PRPB will ensure every agent has a working and reliable radio.
3. Radio Recording System: PRPB will completed the P-25 recording system when the purchase of the radio equipment has been completely deployed.

The following chart summarizes the Radio Coverage initiative and the Steps PRPB will take to implement the initiative.

Initial Tasks and Timing – Radio Coverage

Task	Description	Due Date	Status
1.	Radio Coverage Update		In process
	Activities		
	1.1 Simulation based coverage tests with portable radios.	31 MAR 2021	a. Testing was done in March 2021. b. ████████
	1.2 Pending purchase of new amplifiers, antennae and repeaters for the all the site. Replace existing antennas with	31 DEC 2023	Funding has been requested, but has not been allocated

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
	one that has till down and combiner. Replacing obsolete repeaters (3800) with repeaters (4500) in the P25 system.		
	1.3 Pending purchase for replacement of VHF analogue repeaters in the PRPB interoperability network with P25 digital VHF repeaters. With this update, calls on digital VHF repeaters can be encrypted and attached to the recording system.	31 DEC 2023	a. A proposal for this implementation was submitted pending for funds allocation.
	1.4 Test entire radio network to ensure acceptable coverage and reliability of radio network, and to identify any issues.	29 FEB 2024	Funding has been requested, but has not been allocated
	1.5 Work with vendor to resolve any issues identified.	31 MAR 2024	Funding has been requested, but has not been allocated
	1.10 Oversee the vendor and complete the implementation of new repeaters, antennae, amplifiers.	31 MAY 2024	Funding has been requested, but has not been allocated
2.	**Assignment of portable radios to PRPB officers.**		In process
	Activities		
	2.1 Purchase 2,800 portable radios for the P25 system.	31 MAR 2023	In process a. Contracted company delivered the first 500 radios on February 1, 2023, which were assigned to the rank staff. b. Contracted company delivered 1,350 portable radios which are being programmed, adjusted and updated c. Contracted company delivered 950 portable radios which are being programmed, adjusted and updated to begin their assignment.
	2.2 Purchase 1,700 portable radios for the P25 system.	30 SEP 2023	Purchase pending in ASG and in consultation with the Board.
	2.3 Purchase 1,000 portable radios for the P25 system.	31 DEC 2023	Purchase pending submission by PRPB.
3.	Provide appropriate user training for the radio handsets (Reinforce guideline for the radio handsets).	31 MAY-2023	Completed for handsets already deployed. In process for radio being programmed or in deployment.
4.	Ensure a radio support team is in place with proper knowledge and	31 MAY-2023	Completed

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
	training to support the radio network and handsets.		
5.	Ensure users know where to go for help should they need any support with the radio handsets.	31 MAY-2023	Completed for handsets already deployed. In process for radio being programmed or in deployment.
6.	Deploy and individually assign a radio handset to every officer.	31 MAR 2024	Depend of the acquisition of the radios.
7.	Develop a plan to refresh/replace the radios on a regular lifecycle as recommended by the manufacturer.	31 JUN 2023	In process
8.	**Radio Recording System**		
	8.1 Implement recording platform.	MAY 2018	Complete
	8.2 Develop training.	MAY 2018	Complete
	8.3 Train Communications staff on equipment.	MAY 2018	Complete
	8.4 Deploy system.	MAY 2018	Will be Completed when P-25 radio equipment has been deployed.
	8.5 Determine when next system upgrade is needed.	30 JUN 2023	In process

D. Records Management System/GTE Replacement

PRPB will suspend all development related to the current GTE system and C2S modules (including projects supporting Consent Decree mandates) unless deemed essential to PRPB operations. PRPB will procure and implement a comprehensive, modern Law Enforcement Records Management System (RMS), a mission critical system for PRPB.

Paragraph 221 requires, "PRPD shall develop and maintain an automated record management system and electronic files as part of the Action Plans developed for each subsection above."

A modern RMS should serve as the foundation to enable a law enforcement agency to collect, manage, and produce data that is integral to agency operations. An RMS should provide the ability to complete incident/crime/arrest reports, report crime to the public and the FBI/DOJ, produce copies of reports for those members of the community involved in an incident (e.g., traffic collision reports), maintain the chain of custody of property and evidence, and provide the necessary documentation to file cases for prosecution, and integrate with other data systems to ensure accurate and reliable data.

The Commonwealth and the Parties recognize that the current state of GTE and other modules and applications built by C2S and/or other contractors have not fully satisfied the requirements of the Consent Decree. As such, the Commonwealth will work to

19

IT Corrective Action Plan (Draft)

identify a commercial off-the-shelf RMS that can replace GTE/C2S modules. Should a commercial RMS not be able to provide all Consent Decree required functionality, a plan will be developed to ensure any GTE/C2S modules that will be retained will be fully integrated into the COTS RMS. Data siloes will not be permitted.

The following chart summarizes the RMS / GTE Replacement initiative and the steps PRPB will take to implement the initiative.

Initial Tasks and Timing – RMS

The RMS initiative will be an extensive undertaking. The task list below represents an initial understanding of the tasks needed for implementation and their respective timing. The IT Innovation Task Force should develop detailed tasks to be included in an implementation plan.

Task	Description	Due Date	Status
1.	The Parties will agree upon the list of existing and planned modules that do not require further development, and should remain supported "as is" until such time that they can be replaced with an RMS or other COTS solution	31 MAY 2023	Not Started.
2.	Perform an assessment to purchase or develop an RMS.	30 JUN 2023	Not Started.
	Activities		
	2.1 Contract an RMS Subject Matter Expert (SME) to: (1) help draft an RFI for an RMS, (2) collect and document business and technical requirements for an RMS, (3) draft an RFP, (4) assist with the RFP evaluation and vendor selection process, (5) assist with the development (6) potentially serve as project manager throughout process.	30 APR 2023	Not Started.
	2.2 Develop and release a Request for Information (RFI) or outreach through a vendor community organization to formally determine the availability of, or plans for, Spanish language software from public safety vendors.	30 APR 2023	Not Started.
	2.3 Develop a detailed plan for RMS procurement, based on RFI results, to include a clear delineation between what can be replaced via	30 SEP 2023	Not Started

20

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
	a commercial RMS and what must be retained in either GTE or other in-house contractors to achieve Consent Decree compliance.		
3.	Contract with a System Architect to design the integration architecture between the COTS RMS and any remaining GTE.	31 DEC 2023	Not Started.
4.	IT Planning Committee and Stakeholders review and approve plan for RMS	30 SEP 2023	Not Started
5.	Document functional requirements for an RMS, to include NIBRS certification	30 SEP 2023	Not Started
6.	Document technical requirements for an RMS	30 SEP 2023	Not Started
7.	Release an RFP for an RMS	30 SEP 2023	Not Started
8.	Evaluate vendor proposals for an RMS and select a vendor	30 SEP 2023	Not Started
9.	Contract with the selected RMS vendor	31 DEC 2023	Not Started
10.	Develop a phased RMS implementation plan with selected vendor	31 DEC 2023	Not Started
11.	Implement RMS Phase I - to include NIBRS certification	30 JUN 2024	Not Started

E. Training Technology

Training technology includes two separate and distinct efforts:

1. IT Training: PRPB will ensure that proper training is developed and delivered for every new IT solution that is implemented; and
2. Academy IT: PRPB will update the technology at its Training Academy and maintain and refresh the technology on a regular life cycle.

Training serves as the backbone for every law enforcement agency. When new IT or data systems are implemented, all users must be properly trained. That training must include: a) instruction on how to use the technology or system; b) instruction on how to use the technology or system within the context of the approved policy for that system; c) instruction on how to obtain assistance if they have questions or difficulties when using the technology.

For example, when a law enforcement agency deploys body cameras, they must train officers regarding: a) how to turn the camera on and off; b) when to turn the camera on and off, according to department policy; and c) who to contact when the body camera is not working and how to obtain a replacement camera if needed.

IT Corrective Action Plan (Draft)

Additionally, Academy instructors must be trained in the same, and the training must be incorporated into pre-service training at the Academy.

Police departments must also be able to deliver and track training to ensure employees are current with their training, as policies and procedures evolve, and receive refresher training to regularly exercise their perishable skills. A proper learning management system (LMS) will track all training and certifications, deliver eLearning modules where appropriate, maintain all training curricula and materials; allow the academy to create courses, enroll students and assign instructors.

In addition to a Learning Management System, PRPB will develop and deploy a pre-service training module, a shooting qualifications module, a Field Training Officer (FTO) platform, and an eLearning platform to support Academy Training.

The following chart summarizes the Training Technology initiative and the steps PRPB will take to implement the initiative.

Initial Tasks and Timing – Training Technology

Task	Description	Due Date	Status
IT Training			
1.	Establish an IT training team of qualified instructors.	31 MAY 2023	In Process
2.	Develop IT training for each existing IT and data system.	30 SEP 2023	In Process
3.	Develop IT training for each new IT initiative.	30 JUN 2024	Planning phase
4.	Procure all equipment necessary to deliver training.	30 MAR 2024	In Process
5.	Submit each training to the DOJ and Monitor for review and approval.	31 JUL 2024	In Process
6.	Develop a plan and schedule to deliver each training.	TBA	Subject to the approval of the Monitor and DOJ (see task 5)
7.	Conduct each training according to the schedule.	TBA	Subject to the approval of the Monitor and DOJ (see task 5)
Academy IT			
The following tasks are in direct support of the Training Plan that has been filed with the Court. All tasks will ensure that all IT needed to implement the Training Plan will be provided.			
1.	Review and prioritize IT software and hardware needs of the Academy, to include	30 APR 2023	In Process

22

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
	an LMS, instructor and classroom equipment, and all hardware/software necessary to support the Training Plan.		
2.	Identify software and hardware that is no longer supported or is at end of life	30 APR 2023	In Process
3.	Determine and prioritize the minimum requirements needed by the Academy to provide pre-service and in-service training.	31 MAY 2023	Planning phase
4.	Create a Procurement Plan to replace aging hardware and software	31 MAY 2023	In Process
5.	Utilize prioritized inventory list to request a quotation for replacement assets	31 MAY 2023	In Process
6.	Purchase new equipment	31 AUG 2023	Not Started
7.	Develop an implementation plan to rollout new assets	30 SEP 2023	Not Started
8.	Execute an implementation plan to rollout new assets	31 OCT 2023	Not Started
New PTMS (in support of Training Plan)			
1.	Document requirements	30 NOV 2023	Not Started
2.	Develop and Test PTMS	29 FEB 2024	Not Started
3.	Design and build reports	31 MAR 2024	Not Started
4.	Develop technical manual	30 APR 2024	Not Started
5.	Develop user manual and training materials and policies	31 JUL 2024	Not Started
6.	Submit PTMS Module plans for policies and trainings to DOJ and Monitor for approval	30 SEP 2024	Not Started
7.	Provide training on PTMS	30 NOV 2024	Not Started
8.	Demonstrate DOJ and Monitor and confirm PTMS will meet Consent Decree requirements if built, implemented, and used as designed.	31 DEC 2024	Not Started
Academy IT Recruit Module (to be integrated into PTMS in support of Training Plan)			
1.	Develop, Implement and Integration Cadet Module	29 FEB 2024	Not Started
2.	Design and build reports	31 MAR 2024	Not Started
3.	Develop technical manual	30 APR 2024	Not Started
4.	Develop user manual and training materials and policies	31 JUL 2024	Not Started
5.	Submit Cadet Module plans, policies and trainings to DOJ and Monitor for approval	30 SEP 2024	Not Started
6.	Provide training on PTMS	30 NOV 2024	Not Started
7.	Demonstrate DOJ and Monitor and confirm that module will meet Consent Decree requirements if built, implemented, and used as designed.	31 DEC 2024	Not Started
Academy Shooting Module (SHOOTER) (to be integrated into PTMS in support of Training Plan)			

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
1.	Design, Develop and Integration SHOOTER Module	29 FEB 2024	Not Started
2.	Design and build reports	31 MAR 2024	Not Started
3.	Develop technical manual	30 APR 2024	Not Started
4.	Develop user manual and training materials and policies	31 JUL 2024	Not Started
5.	Submit SHOOTER Module plans, policies, manuals, and trainings to DOJ and Monitor for approval	30 SEP 2024	Not Started
6.	Provide training on PTMS	30 NOV 2024	Not Started
7.	Demonstrate DOJ and Monitor and confirm that module will meet Consent Decree requirements if built, implemented, and used as designed.	31 DEC 2024	Not Started
FTO Platform			
1.	Identify a vendor solution for platform	30 SEP 2023	Not Started
2.	Test FTO platform	31 DEC 2023	Not Started
3.	Design and build reports	30 MAR 2024	Not Started
4.	Develop technical manual	30 MAR 2024	Not Started
5.	Develop user manual and training materials and policies	30 JUN 2024	Not Started
6.	Provide training on platform	30 JUN 2024	Not Started
7.	Demonstrate DOJ and Monitor and confirm that module will meet Consent Decree requirements if built, implemented, and used as designed.	31 DEC 2024	Not Started
eLearning Platform/Online Courses (to be integrated into PTMS in support of Training Plan)			
1.	Identify a vendor solution for platform	30 SEP 2023	Not Started
2.	Document requirements for platform	31 DEC 2023	Not Started
3.	Test eLearning platform	30 MAR 2024	Not Started
4.	Design and build reports	30 MAR 2024	Not Started
5.	Develop technical manual	30 JUN 2024	Not Started
6.	Develop user manual and training materials and policies	30 JUN 2024	Not Started
7.	Provide training on platform	30 SEP 2024	Not Started
8.	Demonstrate DOJ and Monitor and confirm that module will meet Consent Decree requirements if built, implemented, and used as designed.	31 DEC 2024	Not Started
CertiWeb New (Academy Training Plan)			
1.	Develop and implement platform	29 FEB 2024	Not Started
2.	Develop technical manual	31 MAR 2024	Not Started
3.	Develop user manual and training materials and policies	30 APR 2024	Not Started
4.	Demonstrate DOJ and Monitor and confirm that module will meet Consent Decree	31 AUG 2024	Not Started

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
	requirements if built, implemented, and used as designed.		

F. Analytics and Reporting

PRPB will improve its data and analytics capabilities and use modern analytical reporting tools to provide useful data internally and externally.

Paragraph 220 requires, "PRPD shall develop protocols for collecting, analyzing, and reporting the information required by this Agreement. These protocols shall be developed and implemented in coordination with the TCA and shall be approved by the DOJ prior to implementation."

A law enforcement agency's data must be accurate, reliable and accessible to the right people at the right time. Without accurate data, an organization's crime statistics will be called into question. Moreover, management will be unable to make data driven decisions about deployment, crime strategies, and the like.

PRPB contracted with AH-Datalytics to conduct a Gap Analysis focused on the state of PRPB data systems, availability and reliability of data, and ability to use data as it relates to Consent Decree compliance. Following the completion of the Gap Analysis, PRPB has contracted with AH-Datalytics to implement comprehensive management analytics in support of Consent Decree compliance.

The following chart summarizes the Analytics and Reporting initiative that is underway, and the steps PRPB will take to implement the initiative.

Initial Tasks and Timing – Analytics/Reporting

Task	Description	Due Date	Status
1	Onboard data analytics through AH Datalytics. **Activities** 1.1 Complete gap analysis of data analytics need.	MAR 2022	Complete
2	Develop proof of concept data analytics.	SEP 2022	Complete
3	Create continual data analytics product to support.	30 JUN 2024	In process Depending on reporting needs, the due date may be extended.
4	Publish first set of public dashboards.	30 APR 2023	In process
5	Acquire enterprise-wide licensing.	30 APR 2023	In process
6	Develop analytics in conjunction with Reform Office and IT's priority.	30 JUN 2024	In process

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
	Activities - Incorporate data analytics into Consent Decree management meetings such as "ReformStat".		Analytics will be incorporated into ReformStat from the beginning, but ReformStat is envisioned as an ongoing accountability process.
7	Prepare training materials and conduct training and raise awareness.	30 JUN 2024	Not Started
8	Expand analytics to include all aspects of PRPB.	30 JUN 2024	Not Started
9	As RMS is implemented, re-create or modify data products as needed.	30 JUN 2024	Not Started
10	Develop and Implement a Data Management Framework.	31 DEC 2024	Not started

G. Mobility and Situational Awareness

PRPB will improve Agent safety through the implementation of mobile access for Patrol, including situational awareness data and direct access to PRPB applications.

The advent of mobile data computers (MDC's), smartphones, tablets, and other mobile devices have enabled officers to submit and receive critical information from the field, resulting in increased situational awareness, officer safety and various efficiencies in the field.

The following chart summarizes the Mobility and Situational Awareness initiative and the steps PRPB will take to implement the initiative.

Initial Tasks and Timing – Mobility and Situational Awareness

Task	Description	Due Date	Status
Mobile Data Computers (MDCs)			
1.	Identify Team Lead	31 JUL 2023	Planning
2.	Conduct an audit of all existing mobile devices installed in patrol vehicles and other relevant vehicle types (e.g., helicopters).	31 JUL 2023	In process
	Activities 2.1 Vehicle mount installation for mobile applications. 2.2 Full inventory of available vehicles and hardware needed for other vehicles.		In process - 221 have been installed. In Process - Get full inventory of other vehicles that require trays or other mounting equipment.

26

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
3.	Assess gap between total number of mobile users (people who need access to data in the field) and total number of devices available.	30 AUG 2023	Planning
	Activities 3.1 Coordinate with Area supervisors to get the number of users. 3.2 Gather the inventory of existing assigned equipment. 3.3 Review vehicle inventory with the Transportation Director to assess the needs. 3.4 Determine the necessary hardware for further installations and assignment.		Planning Phase On most tasks. In process - As new equipment is installed we are gathering information on existing equipment assigned to the Areas.
4.	Procure required number of mobile devices to ensure everyone who needs access to situational awareness data and other PRPB information systems via a mobile device has it.	30 SEP 2023	Planning
	Activities 4.1 Coordinate with Area supervisors to get the number of users who need access. 4.2 Determine the actual equipment inventory to procure the mobile devices needed. 4.3 Determine necessary budget to acquire the equipment.		Planning
5.	Configure and test mobile device access to PRPB information systems requiring access from the field (e.g., CAD, RMS, NCIC, etc.).	31 DEC 2023	Planning
	Activities 5.1 Prepare the device image with all required settings and software. 5.2 Run the image with all applications and settings. 5.3 Add SIM Card, connect to the Domain. 5.4 Review image installation. 5.5 Test applications and connection.		As equipment is being received and it is to be assigned the steps to install necessary software and SIM cards are being followed.
6.	Provide appropriate user training for the mobile devices.	30 MAR 2024	Not Started
	Activity 6.1. Develop updated training.		a. Review the user training already being provided by the Academy. b. Update the existing training or assist the Academy in creating a new user training.

27

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
7.	Ensure users know where to go for help with the mobile devices.	30 JUN 2023	In process
	Activities 7.1 Every user is informed on how to contact the IT Help Desk for support.		In process
8.	Identify the mobile devices in the IT asset inventory to ensure the devices are maintained and refreshed / replaced on a lifecycle as recommended by the manufacturer.	31 DEC 2023	In process
	8.1 The IT Department maintains an application for the equipment's lifecycle.		In process
Other Mobile Devices (Smartphones, tablets, etc.)			
1.	Document use cases for other mobile devices (e.g., access to body worn video app).	30 JUN 2023	In Process
2.	Identify mobile applications that will be approved for deployment.	30 APR 2023	In process
	2.1 CAD Mobile, RMS, any remaining GTE modules, EIS Source System modules.		a. Mobile applications have been Identified (Cad Mobil, GTE all EIS Modules).
3.	Identify devices that will support all documented requirements.	30 JUN 2023	In process for new devices
	3.1 Devices that support the requirements for mobility.		a. Equipment identified (Laptops and tablets). b. Equipment being provided with specification.
4.	Identify mobile device management solution (MDM) to manage all mobile devices.	31 JUL 2023	In Process
	Activity 4.1 The NPPR has an MDM that is being installed in all new equipment.		a. Testing with Provider
5.	Procure and implement an MDM.	31 JUL 2023	In Process
	Activity 5.1 MDM Implementation.		a. MDM is in testing.
6.	Procure devices and register devices on the network/MDM for provisioning.	31 JUL 2023	In Process
	Activity		a. ██████ is being installed in all mobile devices.
7.	Develop mobile device policy.	31 JUL 2023	Initiation

IT Corrective Action Plan (Draft)

5.0 OTHER EXISTING PRPB IT PROJECTS

In addition to the top 7 IT initiatives, there are several other IT initiatives that PRPB began prior to the development of this Corrective Action Plan. Those initiatives and a task list for each are detailed in the attached Exhibit 3 and hereby incorporated into this Corrective Action Plan.

The task lists contained in this Corrective Action Plan are only a starting point. PRPB will establish teams for each initiative that will focus on hiring/contracting with SMEs with the appropriate skill sets to develop and lead detailed implementation plans for each initiative.

Further, a collaboration period will be included for each initiative to allow for stakeholder review and approval of each detailed implementation plan.

6.0 THE FIRST 90 DAYS

The task lists contained in this Corrective Action Plan are only a starting point. PRPB will establish teams for each initiative that will focus on hiring/contracting with SMEs with the appropriate skill sets to develop and lead detailed implementation plans for each initiative.

Further, a collaboration period will be included for each initiative to allow for stakeholder review and approval of each detailed implementation plan.

The Commonwealth and PRPB will engage in the following next steps over the next 90 days as it begins the implementation of this IT Corrective Action Plan.

A. Governance – The First 90 Days (April-June 2023)
   1. Hire SME to serve as Program Manager to help facilitate governance process, create documentation (including the Governance Oversight and Management Protocol), and facilitate initial IT Planning Committee and PMO meetings
   2. Hold first Executive IT Planning Committee and PMO meetings
   3. PMO submit its first monthly report to the IT Planning Committee
   4. Schedule IT Corrective Action Plan check-in meetings with stakeholders (Monitor, DOJ, etc.)
B. Top 7 Initiatives – The First 90 Days (April-June 2023)
   1. Establish teams and identify accountable leads for each initiative, and develop detailed implementation plans for each.
   2. Develop cost estimates for each IT initiative.
   3. The Parties meet to agree upon the list of existing and planned IT modules/solutions that do not require further development, and should remain supported "as is" until such time that they can be replaced with and RMS or other COTS solution. (See Appendix C)
   4. Determine where SMEs must be hired/contracted to lead or assist teams, and document necessary skill sets for each.

29

IT Corrective Action Plan (Draft)

5. Data Networks team to conduct outreach to existing data network vendor and begin developing a potential scope of work.
6. Radio Coverage team to conduct outreach to radio vendor and begin developing a potential scope of work and project schedule, and secure project funding.
7. Radio Coverage team to conduct an audit of inventory of radio handsets and peripheral equipment (e.g., batteries)
8. Contract with SMEs to document RMS requirements and assist with procurement
9. Contract with SMEs to assist with IT Staffing planning and selections and coordinate with HR.

7.0 HIGH LEVEL SCHEDULE FOR TOP 7 INITIATIVES

The following chart is intended to serve as version 1.0 of a high-level schedule for the Top 7 priority initiatives. This chart will be revised over time, as detailed implementation plans are developed for each initiative.
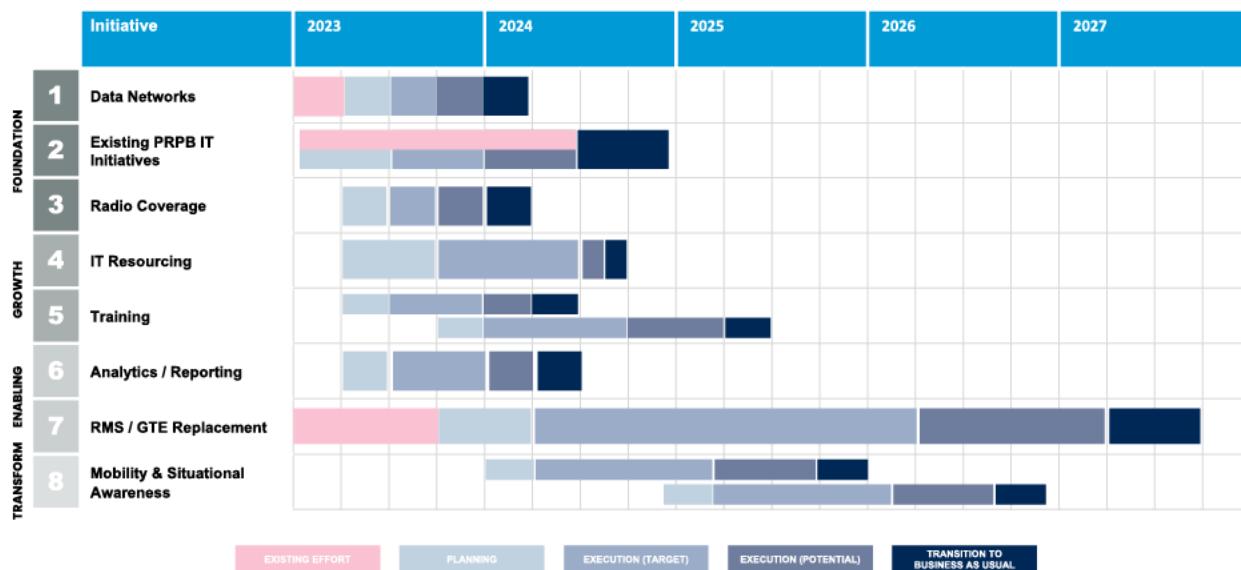
8.0 CONSENT DECREE COMPLIANCE

These initiatives are essential to Consent Decree compliance. A systemic approach to IT governance and IT implementation is needed to create long-lasting improvements to PRPB's IT environment.

Specifically, radio coverage, data networks, and mobility awareness will enable officers and supervisors to have ready access to information, facilitate close and effective supervision, and streamline the process for incident reporting. These are capabilities that are expected of modern-day police departments will help deliver quality policing services to the Commonwealth. An integrated records management system is essential for documenting core aspects of constitutional policing and providing comprehensive data reporting to internal and external stakeholders.

30

IT Corrective Action Plan (Draft)

Additionally, much of the work to implement this IT Corrective Action Plan will also support other non-IT related Consent Decree requirements, as outlined in Appendix A.

Finally, to accomplish these initiatives, and position PRPB for long-term success, Information Technology must be appropriately staffed.

APPENDIX A

The imperative corrections and initiatives in this IT Corrective Action Plan are designed to promote the Commonwealth's compliance with the IT requirements of the Consent Decree. The implementation of these measures and initiatives will also further the Commonwealth's compliance with other substantive requirements, as outlined below.

	CAP Initiative	IT Consent Decree Requirement	Associated Consent Decree Requirements
1.	IT Governance	218 – Establish information systems and use technology to support the Consent Decree's implementation in an efficient and effective manner.	12, 22, 58, 80, 101, 109, 117, 135, 159, 205
2.	IT Resourcing/Staffing	218 – Establish information systems and use technology to support the Consent Decree's implementation in an efficient and effective manner. 224 – Permissively use contracted services related to IT and data collection, entry, and analysis. 289 – Provide or obtain necessary support and resources to enable PRPB to fulfill its obligations under the Consent Decree.	12, 22, 58, 80, 101, 109, 117, 135, 159, 205
3.	Data Networks	218 – Establish information systems and use technology to support the Consent Decree's implementation in an efficient and effective manner. 219 – Collect and maintain necessary data and records. 220 – Develop protocols for collecting, analyzing, and reporting information required by the Consent Decree. 221 – Develop and maintain an automated Record Management System (RMS) and electronic files. 223 – Provide all officers access to National Crime Information Center (NCIC) and develop protocol for the handling and use of NCIC data.	12, 22, 30, 31, 36, 37, 38, 39, 41, 45, 46, 52, 56, 57, 58, 60, 62, 63, 64, 66, 67, 69, 70, 71, 72, 75, 76, 77, 80, 82, 83, 85, 86, 91, 92, 96, 97, 100, 101, 107, 109, 114, 115, 117, 133, 134, 135, 146, 148, 150, 151, 159, 165, 168, 169, 171, 172, 173, 176, 189, 190, 205, 208, 213, 217
4.	Radio Coverage	218 – Establish information systems and use technology to support the Consent Decree's implementation in an efficient and effective manner. 219 – Collect and maintain all necessary data and records to promote officer and civilian safety and other purposes.	33, 36, 38, 43, 49, 57, 66, 67, 139, 169
5.	RMS/GTE Replacement	218 – Establish information systems and use technology to support the Consent Decree's implementation in an efficient and effective manner. 219 – Collect and maintain necessary data and records. 220 – Develop protocols for collecting, analyzing, and reporting information required by the Consent Decree. 221 – Develop and maintain an automated RMS and electronic files.	13, 28, 30, 31, 33, 35, 36, 37, 38, 39, 40, 41, 43, 44, 48, 49, 51, 52, 56, 57, 60, 62, 63, 64, 66, 67, 69, 70, 71, 72, 75, 76, 77, 83, 85, 86, 91, 92, 95, 97, 100, 148, 151, 152, 155, 163, 171, 172, 173, 176, 217
6.	Training Technology	218 – Establish information systems and use technology to support the Consent Decree's implementation in an efficient and effective manner. 219 – Collect and maintain necessary data and records. 220 – Develop protocols for collecting, analyzing, and reporting information required by the Consent Decree.	16, 21, 26, 29, 53, 54, 55, 56, 57, 78, 79, 90, 117, 118, 119, 120, 121, 122, 123, 125, 126, 127, 128, 129, 131, 132, 133, 134, 141, 142, 143, 144, 196, 206, 211
7.	Analytics and Reporting	218 – Establish information systems and use technology to support the Consent Decree's implementation in an efficient and effective manner. 219 – Collect and maintain necessary data and records. 220 – Develop protocols for collecting, analyzing, and reporting information required by the Consent Decree.	13, 26, 28, 30, 31, 34, 35, 37, 39, 40, 41, 45, 46, 51, 52, 56, 57, 60, 62, 64, 76, 83, 85, 86, 91, 95, 97, 100, 131, 134, 147, 148, 151, 153, 154, 155, 157, 171, 176, 179, 208, 217
8.	Mobility and Situational Awareness	218 – Establish information systems and use technology to support the Consent Decree's implementation in an efficient and effective manner. 219 – Collect and maintain necessary data and records. 220 – Develop protocols for collecting, analyzing, and reporting information required by the Consent Decree. 221 – Develop and maintain an automated RMS and electronic files. 223 – Provide all officers access to NCIC and develop protocol for the handling and use of NCIC data.	33, 36, 38, 49, 56, 57, 66, 67, 137, 139

APPENDIX B

Human resources needed to implement Technology Projects

Job Title	Description	Actual	Needed
1. IT Bureau Director (4242 Principal Officer of Analysis development and programming of information systems) (Pending Verification)	Responsible for compliance with the development, implementation, administration and operation of the TCB's IT policy.	1	0
2. IT Bureau Assistant Director (4241 Analysis officer, development and programming of information systems) (Pending Verification)	Assist the Director in the continuity of the projects and services of the Bureau and will replace him in his absence.	0	1
3. Information Systems Specialist (4223 System Information Specialist)	Provide the support and assistance required by those operational units that have information systems and/or need to acquire them to meet the particular, unique and/or special needs of the Agency.	1	1
4. Software and Application Developer (4223 System Information Specialist)	Staff responsible for the development of IT solutions for the Agency that are not covered by external companies.	1	4
5. Database Administrator (4441 Database Administrator)	Manage and provide maintenance to all databases, information systems and applications implemented in the Computer Center	0	2
6. Website Developer (4511 Website Graphic Designer)	Develop and maintain the PRPB website	0	2
7. 4222 Information Systems Analyst	It studies an organization's current information systems and computer procedures, and designs solutions to help the organization operate more efficiently and effectively.	0	1
8. IT Project Manager (5141 Project Management Analyst)	Responsible for initiating, planning, designing, executing, reviewing, controlling and closing the project or projects assigned to it.	2	4
9. Terminal Agency Coordinator (4231 Information Systems Training Specialist)	Comply with the functions established by the CJIS Systems Officer (CSO) and the rules and procedures of the National Criminal Information System (NCIC).	1	4
10. Executive Officer (Contract Management, etc.), (2115 Administrative Officer)	Provide high-level administrative support by conducting research, preparing statistical reports, handling requests for information, and performing office functions such as preparing correspondence, receiving visitors, arranging conference calls, and scheduling meetings.	0	1
11. Division Director (4225 Information Systems Manager)	Plan, organize, implement and maintain the Agency's Computerized Information Systems and the technological teams	0	1

33

IT Corrective Action Plan (Draft)

Job Title	Description	Actual	Needed
	designated in the areas, as well as at the central level, in optimal conditions for the performance of the operational, administrative and investigative tasks of the PRPB.		
12. Assistant Division Director (4424 Assistant Manager of Information Systems)	Assist the Director in the continuity of the projects and services of the Division and will replace him in his absence.	0	1
13. Electronic Information Equipment Operator Supervisor (4421 Information Technology Operations Supervisor)	Responsible for the implementation and maintenance of the Information Systems managed and contained in the Agency's computer center.	1	0
14. Data Communications Coordinator (4541 Network Technical Support Specialist)	Install and provide maintenance to the wired and wireless infrastructure, as well as the electronic devices necessary to distribute the data communication service in the Agency.	0	2
15. 4331 Information Systems Security Officer	Plans and carries out security measures to protect an organization's networks and computer systems.	0	1
16. Information System Security Assistant (4311 Information Systems Security Technician)	~~Plans and implements~~ Execute security measures to protect an organization's networks and computer systems	0	2
17. 4151 Information Systems Technician	Plan the services and maintenance of the equipment, as well as attend to the problems that arise in the different Police Areas related to the data communications network.	4	5
18. Director of Information Systems Services (4223 Information Systems Specialist)	Plan, coordinate, monitor and evaluate work activities related to the services and technical support provided to users of the Agency's information and technology systems.	0	5
19. Technology Coordinator (They would need to respond to the TCB) (4161Technical Support Coordinator)	Collaborate with the Technology Division, in the processes of implementation, development, management and maintenance of both computer systems and electronic equipment assigned to the area.	14 (Currently MPRPB)	14 (Must be Civilian)
20. Alternate Technology Coordinator (They would need to respond to the TCB) (4151 Information Systems Technician)	Assist the Technology Coordinator of the Area in the processes of implementation, development, management and maintenance, both of the computerized systems and the related electronic equipment assigned to the area.	14 (Currently MPRPB)	14 (Must be Civilian)
21. Administrative Officer (Management of the administrative affairs of the two division), (2113 Administrative Assistant)	Perform routine administrative functions, such as drafting documents, scheduling appointments, organizing and maintaining paper and electronic files, or providing information to individuals who contact the Division.	1	2

IT Corrective Action Plan (Draft)

Job Title	Description	Actual	Needed
22. Communications Division Director (3191-C Director of Communications)	Responsible for all the radio communications infrastructure and the electronic equipment used and implemented in it, composed of the microwave network, trunked radio system, conventional repeaters, dispatch consoles, telephone panels and radio units, including the towers, antennas and electric generators of the PRPB.	1	0
23. Communications Division Assistant Director (1173 Supervisor of Communication Systems) (Pending Verification)	Assist the Director in the planning, organization, implementation and maintenance of the Agency's Communications Systems.	0	1
24. Communications Equipment Technician III (1772 Communications Technician Senior)	He will supervise the Telecommunications Infrastructure Groups, Emergency Generators, Telephone Box, Radio Equipment Repairs, Voice and Data Network.	1	2
25. Communications Team Technician I (1771 Communications Technician)	Install, repair and provide maintenance to the wired infrastructure, telephone equipment, as well as the voice and data service of the agency.	2	2
26. Installer of Towers and Antennas (4532 Telecommunications Infrastructure Specialist)	Install, remove, repair, adjust and if necessary change the wired infrastructure of the towers and antennas of the Agency's communications system.	2	4
27. Communications Emergency Plant Technician (1721 Emergency Electric Generator Technician)	Install, repair and maintain in optimal condition the electricity generators that are assigned to the Division, as well as provide support to the electric generators that belong to the Agency of the different districts, seals and units.	2	2
	Total:	52	77

IT Corrective Action Plan (Draft)

APPENDIX C

Modules in development or developed to date to support data collection are listed below. These modules will be evaluated by the Parties and the Monitor to determine which must continue with development, and which do not require further development because they will be replaced with an RMS or other COTS solution.

RMS Core Capabilities – Task/Activities List

Task	Description	Due Date	Status
1.	Call for Service (CAD/CAD Mobile)		In production and implement.
2.	Incident Reporting (Globally Totally Electronic (GTE))	JAN 2019	a. In production and implement since January 2019. b. The systems updates depend on the policies and procedures that changes the forms used in the system. c. Pending for Compliance from DOJ and Monitor.
3.	Crime Information Warehouse (CIW)	JUL 2010	a. In production and implement since July 2010. b. Approved by the Responsible Unit. c. Formal training for the use and management of the system were provided by the SAEA. d. Pending for a Demo and Compliance from DOJ and Monitor.
4.	Case Management (SISCO)	Q4 2023	a. In production and implement since JUN 2017 b. This system has to be updated based on the requirements and needs of the responsible units. c. This system needs to be demonstrated to the DOJ and Monitor for Compliance.
5.	Warrants (NCIC/RCI Warrant Integration)	JUL 1987	a. In production and implement since July 1987. b. The access to these systems is responsible of the CJIS Service Agency (CSA) and liaison by the Terminal Agency Coordinator (TAC).

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
			c. All police areas have personnel trained and certified by CJIS and FBI to access those systems to search for warrants. d. Formal training for the use and management of the systems were provided by the FBI and TAC unit. e. Pending for a Demo and Compliance from DOJ and Monitor.
6.	Arrests Module / Search & Seizure Module (GTE+SISCO)	TBA	a. The forms that collects the data related to the arrests, search and seizure are in production and use since May, 2018 in the GTE System. b. Request for requirements and needs from responsible units to update the GTE and SISCO System. c. GTE and SISCO integration for the arrests, search and seizure forms. d. Update of the GTE and SISCO systems. e. Implement the update of the GTE and SISCO systems. f. Update the training for the use and management of the updated systems. g. Test and approval of the updated systems by the responsible units.
7.	Juvenile Contact	N/A	All applications and modules developed in the PRPB comply with the requirements with the juvenile justice system that requires special handling of information about juveniles, as stated by the Commonwealth state of law.
8.	Crash Reporting (Included in GTE)	DEC 2018	a. Approved by the Responsible Unit. b. In production and implement since December 2018.

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
			c. An API was implemented to share information about crash reports with the Traffic Safety Commission. d. Pending for Compliance from DOJ and Monitor.
9.	Citation (Included in GTE)	APR 2018	a. The forms that collects the data related to the citations for minor offenses are in production and use since April 2018 in the GTE System. b. Pending for revision in the Reform Office.
10.	Field Contact (Stops)	TBA	a. The draft form for field contact (stops) is pending for approval in the Reform Office.
11.	Civil Process (Services)	TBA	a. COPOP modules has part of this functionality. NTC must evaluate to add all the functionalities recommended in the model to the PRPB Systems.
12.	Protection Order & Restraints (COPOP)	AUG 2021	a. In production and implement since AUG-2021. b. Approved by the Responsible Unit. c. Workshops for the use and management of the module was provided by the developer in coordination with the TCB and the Responsible Unit.
13.	Integrations & Interfaces (Internal)	2018 to Present	The PRPB integrates all the internal systems, applications and modules that was requested for the responsible units or been required by the Decree.
14.	Reporting	2016 to Present	The CIW reports and the GTE Systems, as many of the software that is implemented in the PRPB provides the users with a variety of reports to oversees administrative, operational and investigative work. The PRPB will perform

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
			an assessment to address the full compliance with the Decree.
15.	Analytical Support	OCT 2020	a. Contract AH-Datalytics for analytical support are awarded from October 2020. b. Design & develop dashboards to help in the data analysis to support is the systematic process of collecting, collating, analyzing, and disseminating timely, accurate, and useful information that describes patterns, trends, problems, and potential suspects in criminal activity. c. Coordinate demos with the DOJ and Monitor.
16.	Search	TBA	a. Request responsible units to assess and provide the requirements to create a master index to track cases, incidents, citations, reports, permit or license numbers. b. Evaluate the CIW to establish the functionality that allows users to query system.
17.	System Administration	JUL 2010	Verify the system administration of the CIW to oversees is encompasses a wide array of general functions that law enforcement agencies needs to be able to create and query information effectively; to ensure appropriate access to information and system security; and to ensure effective departmental information.
18.	Property & Evidence	TBA	Not Started
19.	Booking (AFIS & CIW)	JUL 2006	a. In production and implement since July 2006 and was updated in 2015. b. Approved by the Responsible Unit. c. Workshops for the use and management of the module

39

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
			was provided by the developer in coordination with the TCB and the Responsible Unit. d. This system needs to be demonstrated to the DOJ and Monitor for Compliance
20.	Permits & Licensing (REAL+)	JUL 2019	a. In production and implement since July 2019. b. Approved by the Responsible Unit. c. Workshops for the use and management of the module was provided by the developer in coordination with the TCB and the Responsible Unit.
21.	Pawn	TBA	Not Started
22.	Fleet Management (FlotaNET)	AUG 2010	a. In production and implement since August 2010. b. Approved by the Responsible Unit. c. Request responsible units to assess and provide the requirements to update the system.
23.	Equipment & Asset Management (ProCon)	APR 2015	a. In production and implement April 2015. b. Approved by the Responsible Unit. c. Request responsible units to assess and provide the requirements to update the system.
24.	Personnel (KRONOS)	JUN 2021	a. In production and implement since June 2021 b. Approved by the Responsible Unit. c. Pending for Compliance from DOJ and Monitor.
25.	Offender Registration (NCIC)	APR 2014	a. In production and implement since APR-2014. b. Approved by the Responsible Unit. c. Formal training for the use and management of the system were provided by

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
			the PRDOJ, CJIS, FBI and TAC unit.

RMS Master Indices – Task/Activities List

Task	Description	Due Date	Status
1.	Master Indices (CIW)	JUL 2010	a. In production and implement since July 2010. b. Approved by the Responsible Unit. c. Request responsible units to assess and provide the requirements to update the system.
2.	Master Name Index (NMI)	TBA	Request responsible units to assess and provide the requirements to update the system.
3.	Master Vehicle Index (NVI)	TBA	Request responsible units to assess and provide the requirements to update the system.
4.	Master Property Index (NPI)	TBA	Request responsible units to assess and provide the requirements to update the system.
5.	Master Location Index (NLI)	TBA	Request responsible units to assess and provide the requirements to update the system.
6.	Master Organization Index (NOI)	TBA	Request responsible units to assess and provide the requirements to update the system.

RMS External Interfaces – Task/Activities List

Task	Description	Due Date	Status
12.	Computer Aided Dispatch (CAD) System.	APR 2023	In progress
	Activities		
	13. Acquire and implement the updated version of the CAD System (DispatchNow 3.0).	JAN 2019	a. Approved by the Responsible Unit. b. In production and implement since January 2019. c. Pending for Compliance from DOJ and Monitor.

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
	14. Updated version of the CAD System (DispatchNow 3.0) training.		a. Workshops for the use and management of the module was provided by the developer in coordination with the TCB. b. Formal training for the use and management of the module from the Academy are not provided. Waiting for the Academy to offer the formal training. This training is related to the General Order 600-621.
15.	Corrections	TBA	Not started
16.	Juvenile Assessment / Detention Centers	TBA	Not started
17.	Prosecutor (Case Submission)	TBA	a. In production and implement. b. The access to this system belongs to the PRDOJ and the responsible in the PRPB is the Terminal Agency Coordinator (TAC). c. All police areas have personnel trained and certified by the PRDOJ to access, partially, the system. d. Formal training for the use and management of the system were provided by the PRDOJ and TAC unit.
18.	Courts	TBA	Not started
19.	Information Sharing (State – RCI & Federal - NCIC)	JUL 1987	a. In production and implement since July 1987. b. The access to this system belongs to the PRDOJ, CJIS, FBI and the responsible unit in the PRPB is the Terminal Agency Coordinator (TAC). c. All police areas have personnel trained and certified by the PRDOJ, CJIS and FBI to access those systems. d. Formal training for the use and management of those systems were provided by

IT Corrective Action Plan (Draft)

Task	Description	Due Date	Status
			the PRDOJ, CJIS, FBI and TAC unit.
20.	Jail Management System	TBA	Not started